IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

APPLE INC., Plaintiff, v. MASIMO CORPORATION and SOUND UNITED, LLC, Defendants.	)	C.A. No. 22-1377-MN-JLH **JURY TRIAL DEMANDED**
MASIMO CORPORATION, Counter-Claimant, v. APPLE INC., Counter-Defendant.	)	
APPLE INC., Plaintiff, v. MASIMO CORPORATION and SOUND UNITED, LLC, Defendants.	)	C.A. No. 22-1378-MN-JLH **JURY TRIAL DEMANDED**
MASIMO CORPORATION and CERCACOR LABORATORIES, INC., Counter-Claimants, v. APPLE INC., Counter-Defendant.	)	

Re: Apple Inc.'s Letter Brief In Support Of Joint Motion To Resolve PO Disputes

Dear Judge Hall:

Plaintiff Apple Inc. ("Apple") respectfully submits this letter in response to the Court's May 24, 2023 Order setting a discovery dispute teleconference. *See* 1377 Case, D.I. 101; 1378 Case, D.I. 90. The parties have four disputes related to their proposed protective order: (1) the extent to which materials designated under the protective order ("Protected Material") may be exported outside of the United States; (2) whether to implement a patent-acquisition bar; (3) whether the parties may show Protected Material to any of the producing party's employees during their depositions, regardless of those employees' prior access to such materials or having been designated regarding the subject matter of the materials; and (4) whether the parties must implement multifactor authentication to protect and prevent unauthorized access to another party's Protected Material. The parties' competing proposals on those issues are shown in Exhibit A, with Apple's proposed additions and deletions shown in redline.

I. The Court Should Prohibit Exportation Of Protected Material Subject To A Meet And Confer Requirement If Circumstances Requiring Exportation Arise (Section 6(c)).

Apple proposes that Protected Material should not be exported outside the United States or to any foreign national. This is necessary to ensure compliance with United States Export Administration regulations and to protect the parties' sensitive information. Apple's proposal is critical in view of the heightened risk of misuse and unauthorized access of information maintained abroad, differing views of business sensitivity and privacy across foreign jurisdictions, and the potential inability to enforce the protective order in foreign jurisdictions.[1] The provision should not impose any burden on Masimo, given that all Masimo's counsel are located in the United States and all alleged conduct occurred in the United States. Indeed, across multiple meet-and-confers, Masimo has not provided any reason it needs to send Apple's (or any non-party's) highly sensitive information abroad. And, to the extent case developments do require depositions or experts or travel outside of the United States, the parties would meet and confer on the scope of specific materials for which export would be necessary. To date, Masimo has not identified ***any*** witness or expert that this proposal would affect, or any known reason for exportation.

II. The Court Should Adopt A Patent Acquisition Bar (Section 6(b)).

While the parties agree on the necessity of a patent prosecution bar for individuals with access to Attorneys' Eyes Only or Source Code information, Apple requests that the prosecution bar equally extend to patent acquisitions because the rationale supporting a patent prosecution bar applies equally to patent acquisitions. Just as patent prosecution involves the risk that an attorney might use the disclosing party's confidential information to procure patent rights in new and

[1] Other courts have found similar arguments compelling and have enacted similar export controls. *See, e.g., Parallel Networks, LLC, v. Barracuda Networks, Inc.*, CA. No. 13-1412-LPS, D.I. 28 (D. Del. July 31, 2014) (Ex. B); *Id.*, D.I. 30 (Ex. C); *ReefEdge Networks, LLC v. Aruba Networks Inc.*, C.A. No. 12-1042-LPS, D.I. 49 at 33-34 (D. Del. Sept. 8, 2013) (Ex. D); *Kewazinga Corp. v. Google LLC*, No. 1:20-CV-1106-LGS, 2020 WL 2129393, at *11 (S.D.N.Y. May 5, 2020); *Taction Tech., Inc. v. Apple Inc.*, No. 21-CV-00812-GPC-JLB, 2021 WL 4150342, at *3 (S.D. Cal. Sept. 13, 2021); *WAPP Tech Limited Partnership v. Wells Fargo Bank, N.A.*, Case No. 4:21-cv-00671-ALM, D.I. 118 (E.D. Tex. August 1, 2022) (Ex. E); *Summit 6 LLC v. HTC Corporation*, Case No. 7:14-cv-14, D.I. 115 (N.D. Tex. June 26, 2014) (Ex. F).

pending applications based on that party's confidential information, so too can that attorney leverage the opposing party's confidential information in the course of assisting in buying patents. In both situations, the attorney who has had access to the adversary's confidential information is being asked to provide advice to the client that could result in the client having new patent claims that can be asserted against the adversary. *See Telebuyer, LLC v. Amazon.com, Inc.*, No. 13-CV-1677, 2014 WL 5804334, at *7 (W.D. Wash. July 7, 2014) ("Patent acquisition creates the same risks of inadvertent use as patent prosecution, in that 'litigation counsel may consciously or subconsciously use . . . confidential information to advise a client on which patents to acquire.'") (quoting *EPL Holdings, LLC v. Apple Inc.*, No. 12-04306, 2013 WL 2181584, at *4 (N.D. Cal. May 20, 2013)). Furthermore, Apple's proposal is narrowly tailored to only impact acquisitions related to a party or its affiliates. Masimo has failed justify its opposition to an acquisition bar.

III. The Court Should Limit Persons Who Can See Protected Materials At A Deposition To Those Who Had Prior Access (Sections 8(b)(iv), 9(b)(iii), 10(c)(iii)).

Apple proposes that materials designated as "Confidential," "Confidential – Attorneys' Eyes Only," and "Confidential – Outside Attorneys' Eyes Only – Source Code" cannot be shown to witnesses, such as at deposition or in hearings, unless that witness is identified on the designated material as an author, addressee, or recipient of the material in question, or unless there is other indicia indicating the witness has seen or had access to the material previously. Apple further proposes an exception to this rule if the witness has been designated under FRCP 30(b)(6) to testify on behalf of the Producing Party on the subject matter of the material in question, ensuring Masimo will get an opportunity to ask about any potentially relevant documents. (*See* Sections 8(b)(iv)(2), 9(b)(iii)(2), 10(c)(iii)(2).) Masimo's proposal—that ***any*** employee of the Producing Party be allowed access to the material—would frustrate Apple's efforts to enforce the security of its information within Apple. Like many companies, Apple does not make ***all*** internal company information available to ***all*** its employees.[2] Rather, Apple limits access to various types of information based on seniority, position, and other factors. By way of example, Masimo has not provided a rationale for why it should be able to show an Apple employee top-secret source code without first establishing that the employee has had access to that information previously, which is easily discernable (e.g., through preliminary questioning during depositions). Masimo should not be allowed to use litigation as an end-run around a company's own internal access restrictions simply for a tactical advantage at a deposition, especially when there is likely little value in asking witnesses to speculate about materials which they have never seen. Apple could not adequately prepare its witnesses for such tactics without violating its own internal access restrictions.

IV. The Court Should Require Multifactor Authentication To Access Protected Material (Section 14(a)).

Apple asks for a common-sense security measure to protect all confidential information produced in the case: Multi-Factor Authentication (MFA). Organized criminal groups and hostile state actors are perpetrating data security breaches with growing frequency; law firms and their vendors have increasingly become targets of these attacks. The number of breaches increased by

[2] Other courts have enacted restrictions similar to Apple's proposal. *See, e.g., TOT Power Control, S.L. v. Apple Inc.*, C.A. No. 21-1302-MN, D.I. 53 at 13 (D. Del. Jan. 17, 2023) (Ex. G); *GKWF, Inc. v. Aquachem, Inc.*, No. 8:08-cv-01596-SCB-MAP, D.I. 17 at 11 (M.D. Fl. Jan. 26, 2009) (Ex. H); *Wi-LAN, Inc. et al. v. LG Electronics, Inc. et al.*, No. 3:17-cv-358-BEN-MDD, DI. 47 at 6 (S.D. Cal. Nov. 7, 2017) (Ex. I).

17% in 2021; and 24.9% of ransomware attacks in Q1 of 2021 targeted small and medium sized law firms.[3] Given this evolving threat, protective orders must too evolve.[4]

MFA has been called by the U.S. Government "the single most important thing Americans can do to stay safe online."[5] Indeed, the federal judiciary requested congressional funding for enterprise-wide MFA this fiscal year.[6]

Apple's proposed changes to the protective order incorporate the definition of MFA used by the National Institute of Standards and Technology. This requirement does not impose an undue burden, and any firm that is maintaining a party's highly sensitive information has or ought to have the capabilities in place to comply. Indeed, a party could satisfy this MFA requirement simply by registering users' computers with their organization (*e.g.*, law firm or vendor) as trusted devices, after which they can access protected materials with a password. This reasonable process is more secure than passwords alone[7] and is used commonly across corporate America and on the Internet.

In this matter, Apple has already agreed to produce (and may be required to produce more) sensitive data—such as financial figures; internal documents referring to product specifications; product development and industrial designs; and highly confidential IP licenses—all of which, if obtained by bad actors, could materially harm Apple's competitive and business interests. That data—as well as Defendants' data—should be safeguarded with the reasonable, mutually applicable security protocol of MFA.

Respectfully,

/s/ David E. Moore

David E. Moore

DEM:nmt/10836215

Enclosures
cc: Clerk of Court (via hand delivery)
Counsel of Record (via electronic mail)

---

[3] *See, e.g.*, *Why Cybersecurity Should Be Top of Mind in 2022*, JDSUPRA (Jan. 27, 2022), https://www.jdsupra.com/legalnews/why-cybersecurity-should-be-top-of-mind-1297423

[4] *E.g.* Robert Hilson, *Why the archaic process of eDiscovery is vulnerable to hacking and data breach*, LOGIKCULL (Feb. 8, 2017), https://www.logikcull.com/blog/archaic-process-e-discovery-vulnerable-hacking-data-breach.

[5] Jen Easterly, Director, *Next Level MFA: FIDO Authentication*, Cybersecurity & Infrastructure Security Agency (Oct. 18, 2022), https://www.cisa.gov/news-events/news/next-level-mfa-fido-authentication; *see also*, *e.g.*, 16 C.F.R. § 314.4 (FTC standards for safeguarding information).

[6] *See The Judiciary Fiscal Year 2023 Congressional Budget Request: Judiciary Information Technology Fund*, at 11.8, Admin. Office of the U.S. Courts (Mar. 2022), https://www.uscourts.gov/sites/default/files/fy_2023_congressional_budget_request/FY%202023%20Congressional%20Budget%20Request/11a%20-%20Judiciary%20Information%20Technology%20Fund.pdf.

[7] *See Multifactor Authentication*, CISA, cisa.gov/mfa ("Malicious cyber actors are increasingly capable of phishing or harvesting passwords to gain unauthorized access.").